IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF:	
14 HARD DRIVES, ONE CANON VIDEO CAMERA WITH SD CARD, AND ONE GOVERNMENT OWNED HEWLETT PACKARD LAPTOP COMPUTER, AS DESCRIBED IN ATTACHMENT A	**MISC. NO. 17-2148 TJS** **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

INTRODUCTION

I, Ricardo Solis, am a Special Agent (SA) with the Naval Criminal Investigative Service (NCIS), Resident Agency Patuxent River, Maryland, being duly sworn, depose and state as follows: I have been a Special Agent (SA) with NCIS since September 02, 2007. I currently investigate criminal violations of federal, state and local laws, as well as the Uniform Code of Military Justice ("UCMJ"). I gained investigative experience first by attending the Federal Law Enforcement Training Center ("FLETC"), receiving training in conducting said investigations which include legal, operational, and tactical considerations. Additionally, while employed as a Federal Law Enforcement Officer I continued to receive additional training by attending numerous state and local training, workshops, and seminars as well as other federally supported training evolutions ranging from homicide, narcotics, sexually motivated criminal activities, and financial crimes. Prior to NCIS, I held employment with the Department of Homeland Security, Immigration and Customs Enforcement and with the El Paso Police Department in Texas. I conduct a wide range of criminal investigations to include homicides, assaults, rapes, larceny, weapons possessions, narcotics, child pornography, and counter intelligence concerns. While

employed in a law enforcement capacity I have made countless arrests for the aforementioned criminal activities and participated in the execution of numerous search and seizure warrants authorized via Federal and State Warrants as well as Military Command Authorization for Search and Seizure ("CASS"). As a federal agent, I am authorized to investigate violations of laws of the United States and is a law enforcement officer with authority to execute warrants issued under the authority of the United States. This affidavit is made in support of an application for a warrant to search the following electronic devices (collectively, the "TARGET DEVICES"), which are located in the District of Maryland:

a. **Fourteen hard drives of different brands, one Canon video camera with SD card, and one government owned Hewlett Packard laptop computer.**

As further described in Attachment A and incorporated herein by reference.

1. The listed items are to be searched for evidence of violations of Title 18, United States Code, Section 1801 (Video Voyeurism) (referred to as the "TARGET OFFENSE").

2. The statements in this affidavit are based in part on information provided by statements obtained by Detective Michael Theesen of the Naval Air Station (NAS) Patuxent River, Maryland Base Police and on my experience and background as a Special Agent of NCIS. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code, Section 1801 (Video Voyeurism), are located within the TARGET DEVICES.

STATUTORY AUTHORITY

3. This investigation concerns alleged violations of United States Code, Section 1801, Video Voyeurism. Title 18, United States Code, Section 1801, states **(a)** Whoever, in the

special maritime and territorial jurisdiction of the United States, has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined under this title or imprisoned not more than one year, or both.

(b) In this section— **(1)** the term "capture", with respect to an image, means to videotape, photograph, film, record by any means, or broadcast; **(2)** the term "broadcast" means to electronically transmit a visual image with the intent that it be viewed by a person or persons; **(3)** the term "a private area of the individual" means the naked or undergarment clad genitals, pubic area, buttocks, or female breast of that individual; **(4)** the term "female breast" means any portion of the female breast below the top of the areola; and **(5)** the term "under circumstances in which that individual has a reasonable expectation of privacy" means— **(A)** circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or **(B)** circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place. **(c)** This section does not prohibit any lawful law enforcement, correctional, or intelligence activity.

PROBABLE CAUSE

4. On July 12, 2017, NCIS Resident Agency Patuxent River, Maryland was notified by NAS Patuxent River Base Police that Daniel Fasci, a civilian U.S. Navy employee, had been detained in Building 2855 on board NAS Patuxent River, MD for installing a video camera underneath the desk of a female U.S. Navy employee. The camera was in an inconspicuous area to the rear left of the desk, and was detected by an information technology contractor while

doing work at the desk. It was in a position to record parts of the body of the user of the desk in which she had a reasonable expectation of privacy. The user of the desk denied knowing what the video camera was or anything about the video camera. A command-wide email was put out to employees asking if anyone had knowledge of the camera. Daniel Fasci came forward and admitted that it was his camera. Daniel Fasci provided Detective Michael Theesen with a written statement where he admitted that he installed the found camera on Jul 11, 2017 and had obtained photographs and video of at least five other female victims since 2013. Fasci signed a Permissive Authorization for Search and Seizure form where he agreed to provide Detective Theesen with numerous hard drives where he has downloaded videos and photographs that he has obtained of other female victims. Fasci also admitted to going to the NAS Patuxent River base swimming pool and videotaping females that were at the pool. On July 12, 2017 at approximately 1720 hours, Detective Theesen and I entered the residence located at 45930 N. Greens Rest Drive, Great Mills, Maryland, with Fasci's permission, and proceeded to the office area of the residence. Fasci provided Detective Theesen fourteen hard drives, a video camera, and his government issued laptop computer. Those items are now stored at the NCIS Patuxent River Resident Agency, 47372 Buse Road Building 469, Patuxent River, Maryland 20670.

5. Based on my training and experience, and conversations with other law enforcement officers I am aware that it is common for offenders of these violations to maintain large digital collections of movies and images. These individuals often maintain their collections for long periods of time and are known to take their collections with them when relocating, either temporarily or permanently. Due to the compact and portable nature of laptop computers, tablet computers, desktop computers, cellular telephones, cameras, portable hard drives, thumb-drives, and other devices capable of storing and transmitting electronic files, individuals who are

associated with voyeurism can easily transport their collections on, or near, their person so as not to be away from it for a prolonged period of time.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

5. Based on my knowledge, training, and experience, I know that electronic devices – such as the TARGET DEVICES described in Attachment A – can store information for long periods. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information sometimes can be recovered with forensic tools.

6. There is probable cause to believe that, despite the passage of time, the items set forth in Attachment B may be found on the TARGET DEVICES for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what is has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache".

7. *Forensic Evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how the electronic devices were used, the purpose of their use, who used them, and when they were used. There is probable cause to believe that this forensic electronic evidence might be in/on the TARGET DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the

times the computer was in use. Cellular telephone and computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when they were used.

d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw and accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a hard drive or computer is evidence may depend on other information stored on the hard drive or computer and the application of knowledge about how a hard drive or computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when it was used, sometimes it is necessary to establish that a particular thing is not present on the storage medium.

8. *Nature of Examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant that I am applying for would permit the examination of electronic devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

9. Based upon the above information, I believe that the TARGET DEVICES described in Attachment A likely contain evidence, fruits, and/or instrumentalities of crimes associated with the aforementioned Video Voyeurism offense. Based on the foregoing facts, as well as the ability of a forensic analyst to find data long after it has been deleted, and the increased storage capacity of computers over time, probable cause exists that evidence, fruits, and instrumentalities of these offenses will be found in/on the TARGET DEVICES, notwithstanding the passage of time. Therefore, I requests that this Court issue warrants for the TARGET DEVICES described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

CONCLUSION

10. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located in the items to be searched described in Attachment A. I respectfully request that this Court issue a search warrant for the TARGET DEVICES described in Attachment A, which authorizes the search for and seizure of the items described in Attachment B.

11. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain

17-2148TJS

a list of only the tangible items recovered from the TARGET DEVICES. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

I declare under the penalty of perjury that the foregoing is true and accurate.

Special Agent Ricardo Solis
Naval Criminal Investigation Service

Sworn and subscribed before me
This 8th day of August, 2017

Timothy J. Sullivan
United States Magistrate Judge

17-2148TJS

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

The items seized and listed below (collectively, the "TARGET DEVICES"), which are currently secured within the NCIS Patuxent River Resident Agency, 47372 Buse Road Building 469, Patuxent River, Maryland 20670.

a. **Black 3TB Toshiba Hard Drive Serial Number 55B4LWLASU17**

b. **Black Seagate 5TB Expansion Desktop Drive Serial Number NA4KRDKZ**

c. **Black 5TB Hard Drive Serial Number NA7EVNCM**

d. **Black 5TB Hard Drive Serial Number NA7ESPSP**

e. **Black Canon Vixia HF R500 Video Camera Serial Number 802854206929 with 256 GB Sony SD Card**

f. **Silver 3TB Hitachi G/Drive G/Technology Hard Drive Serial Number YHJD75YA**

g. **Silver Western Digital My Book Studio Hard Drive Serial Number WCAWZ3067703**

h. **Black Western Digital My Book Hard Drive Serial Number WCC4N4TZ37XY**

i. **Gray IOMEGA Hard Drive Serial Number 97A922222B**

j. **White Seagate 8TB Backup Plus Hub for MAC Hard Drive Serial Number NA8TH4W5**

k. **White Seagate 8TB Backup Plus Hub for MAC Hard Drive Serial Number NA8TH4LX**

l. **White Seagate 8TB Backup Plus Hub for MAC Hard Drive Serial Number NA8TH4W7**

m. **Black Western Digital Hard Drive Serial Number WMC1T2929602**

n. **Silver Maxtor 200GB Hard Drive Serial Number B41ZNZAH**

o. **Silver G-Technology 1TB Hard Drive Serial Number HD2SUXAC**

p. **Silver Elitebook 8470P Hewlett Packard NCMI Laptop Asset #5100373013 Serial Number MXL30612PN**

17-2148TJS

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence and instrumentalities of any violations of 18 U.S.C. § 1801 Video Voyeurism, including the following:

1. Any and all images as defined under 18 U.S.C. § 1801;

2. Any and all notes, documents, records, or correspondence pertaining to the possession, transport, distribution, receipt, or production of images as defined under 18 U.S.C. § 1801, such as communications with individuals seeking to distribute, produce, or receive these images.

3. Any and all data that could be used to identify persons, dates/times, and devices involved in transmitting, transporting, receiving, or possessing, through interstate commerce including by U.S. Mails or by computer, any images as defined under 18 U.S.C. § 1801, as well as any and all data that could be used to identify the victims of those crimes (such as photos, names, addresses, etc.).

4. Any and all data that could be used to identify persons, dates/times, and devices involved in transmitting, transporting, receiving, or possessing, through interstate commerce including by U.S. Mails or by computer, any images as defined under 18 U.S.C. § 1801, as well as any and all data that could be used to identify the victims of those crimes (such as photos, names, addresses, etc.).

5. Any and all records, documents, invoices, and materials that concern any accounts with any Internet Portal such as Google, Inc., Microsoft, Facebook, Dropbox, etc..

6. Evidence indicating the user's state of mind as it relates to the crimes under investigation within this warrant.

7. Credit card information, bills, and payment records associated with subscriptions/use of Internet Portals;

8. Evidence of routers, modems, and network equipment used to connect the TARGET DEVICES to the Internet and/or other TARGET DEVICES (for example, to show that a TARGET DEVICE was used to transport images to another device, such as a home computer);

9. Any and all electronic diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with victims visually depicted, as defined in 18 U.S.C. § 1801.

10. Documents, data and other records regarding ownership and/or possession of the TARGET DEVICES:

a. evidence of who used, owned, or controlled the TARGET DEVICES at the time that the images were produced, received, distributed, or possessed, including when such images were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat", instant messaging logs, photographs, and correspondence;

b. evidence of software (or the lack of such software) that would allow others to control the TARGET DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

17-2148TJS

c. evidence of computer-forensic programs (and associated data) that are designed to eliminate data from the TARGET DEVICES;

d. evidence of the times the TARGET DEVICES were otherwise used;

e. passwords, encryption keys, and other devices that may be necessary to access the TARGET DEVICES;

f. documentation and manuals that may be necessary to access the TARGET DEVICES or to conduct a forensic examination of the TARGET DEVICES;

g. and contextual information necessary to understand the evidence described in this attachment.